ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

February 19, 1998

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
DIRECTORS OF THE DEFENSE AGENCIES
CO-CHAIRS, INTELLIGENCE SYSTEMS BOARD

SUBJECT: Defense Message System (DMS) Policy Guidance Update

As we proceed on an aggressive DMS implementation schedule (to include Automatic Digital Network (AUTODIN) closure), we must assure the fielding of a robust system that supports tactical/deployable elements, sustaining base, and intelligence communities. To ensure success, we need total community cooperation to provide for life cycle support, critical AUTODIN closure activities, and adherence to recommended connection criteria and engineering practices. This memorandum specifically addresses:

- Elimination of Data Transfer Traffic on AUTODIN (Attachment 1);

- Funding Responsibilities for the DMS: Fiscal Years 2000 - 2004 (Attachment 2);

- Recommendations for Defense Information Systems Network (DISN) Connection Criteria and Engineering Practices to Ensure a Robust DMS (Attachment 3).

DMS has met critical milestones and promises to meet all Joint Staff validated requirements. Continued commitment and cooperation will ensure further success in fielding this critical command, control and intelligence capability in support of our warfighters and a rapid phase-out of AUTODIN.

This memorandum is intended to provide sufficient policy guidance until the DMS directive, currently in staffing, is issued. My point of contact is Ms. Oma Elliott, who is assigned to the office of the Deputy Assistant Secretary of Defense for Command, Control and Communications, telephone: (703) 697-7627/695-7181; DSN: 227-7627/225-7181; email: oma.elliott@osd.pentagon.mil.

Anthony M. Valletta

Anthony M. Valletta
(Acting)

Attachments

cc:
DISA/DMS/PMO
IC DMS Management Office

ELIMINATION OF DATA TRANSFER TRAFFIC ON AUTODIN

Timely closure of AUTODIN requires each Service and Agency to develop a transition plan for redirecting critical non-messaging traffic to other transmission means. A status report on implementation of those plans is due to the DMS Implementation Group within 60 days of the date of this memorandum. Although progress has been made in the elimination of bulk data transfer traffic from AUTODIN (in keeping with earlier guidance), applications continue to use AUTODIN for data transport at the present time. The primary objective of these plans must be to remove all data pattern traffic from AUTODIN by September 1999.

ATTACHMENT 1

FUNDING RESPONSIBILITIES FOR THE DEFENSE MESSAGE SYSTEM (DMS): FISCAL YEARS 2000-2004

This attachment provides the Military Departments, Intelligence Community, and Defense Agencies with a methodology for defining their FY 2000-2004 DMS program (to include staffing) requirements. DMS is a service provided by the Defense Information Infrastructure (DII). Thus, the cost recovery and life cycle maintenance (LCM) concepts within the Defense-wide Capital Fund have some similarity to the Defense Information System Network (DISN).

As the Department of Defense's integrated, common messaging service, DMS must be flexible and interoperable between our Services/Agencies, the Intelligence Community, Federal Agencies, and our Allies. Hence, we must plan, develop, and fund for a common electronic messaging service from the National Command Authority (NCA) to the foxhole. Although viewed as an application layer service, DMS requires hardware, software, procedures, manpower, and training resources to ensure its successful implementation.

- The Defense Information Systems Agency (DISA) has overall program responsibility and provides all strategic, collateral infrastructure services and interfacing requirements between the strategic and non-strategic services (i.e., local enclave, special purpose areas, and tactical/deployable environments).
- The Joint Staff will ensure the Joint Communications Support Element (JCSE) is fully equipped to support at least two joint task forces (JTFs), to include the associated strategic and component interfaces and all communications pipelines (including communications for intelligence systems) to any JTF headquarters, consistent with CJCSI 6110.01, January 25, 1996, subject, "Controlled Tactical Communications Assets."
- The Intelligence Community will ensure similar infrastructure service (to include the tactical/deployable enclave) supporting special compartmented information (SCI) is available for the Department and the national Intelligence Community.
- The Military Departments and Defense Agencies are responsible for their respective Service/Agency requirements (such as bases/posts/camps/stations and tactical/deployable enclaves).
- Finally, DISA, in coordination with the Intelligence Community, is responsible for maintaining configuration management and interoperability throughout the DMS architecture.

ATTACHMENT 2

Detailed guidance on the critical roles and responsibilities for the funding, implementation, operation and LCM of DMS (which includes the strategic/common backbone infrastructure, Service/Agency infrastructure; SCI infrastructure (to include tactical/deployable enclaves); and the collateral tactical/deployable infrastructure) is provided below:

Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD(C3I))

- Provide programmatic, policy, and acquisition guidance and oversight for DoD messaging services (includes both DMS and AUTODIN), as required.
- Serve as functional sponsor.

The Joint Staff

- Review DMS actions for consistency with validated messaging requirements.
- Validate DMS operational requirements.
- Provide assistance in delineating funding responsibilities between joint/common and Service/Component unique requirements within a Headquarters, Joint Task Force and the strategic/common service backbone.
- Review Service/Component programs for compliance with integration and interoperability messaging requirements.
- Serve on the DMS Configuration Management Board (DMS CMB).
- Update joint doctrine/publications, as required.

Intelligence Community

- Provide operational management and control of the Department's messaging service for the intelligence portion (non-collateral).
- Provide, operate, and maintain the intelligence portion of the DMS infrastructure (i.e., special compartmented networks (to include tactical/deployable)) until SCI and collateral infrastructures can be combined as defined in the target architecture.
- Represent the IC on the DMS CMB.
- Ensure the intelligence portion of the Department's messaging service is in compliance with approved and validated requirements.
- Manage the intelligence portion of the DoD-wide implementation of DMS.
- Ensure the performance and accreditation criteria for user-provided infrastructure components meet IC requirements.
-

- Provide, operate, and maintain Certification Authority Workstations (CAWs) for the Intelligence Community.
- Designate a single point of contact for coordination.

Defense Information Systems Agency

- Provide operational direction and management control of the Department's collateral messaging service.
- Provide, operate, and maintain the joint/common, collateral Global DMS infrastructure until SCI and collateral infrastructures can be combined as defined in the target architecture.
- Ensure the Department's messaging service is in compliance with approved and validated requirements, per the Joint Chiefs of Staff (JCS).
- Establish and convene the DMS CMB.
- Coordinate DOD-wide implementation of DMS.
- Perform DMS compliance test and evaluation of DMS components.
- Perform system-wide engineering and integration, modeling, and simulation.
- Provide and install the initial CAWs to support the DMS community of users (NOTE: Services/Components can acquire additional CAWs, if desired).
- In coordination with ASD(C3I), maintain oversight DMS acquisition.
- Serve as DoD registration authority.
- Participate in NSA's Multi-Level Information System Security Initiative (MISSI) CMB.

Military Departments, Defense Agencies

- Maintain and ensure an executable program (both funding and manpower) for their respective Service/Agency requirements (such as bases/posts/camps/stations and tactical/deployable enclaves throughout the DMS implementation) which includes requirements within the strategic/joint, Service/Agency unique, intelligence, and tactical/deployable environments.
- Ensure Service and Agency portions of the DMS phase-in planning and AUTODIN phase-out planning is current, executed on schedule, and consistent with validated requirements and overall DoD program milestones.
- Ensure user-provided software and hardware components meet DMS compliance and interoperability criteria as defined in DoD messaging.
- Provide, operate, and maintain all user components (see definitions below).
- Provide, operate, and maintain non-strategic, collateral DMS infrastructure (i.e., bases/posts/camps/stations and tactical/deployable enclaves).

- Provide operational management of assigned DMS components in accordance with approved DMS operational policy and procedures.
- Identify sub-registration authority to the DoD registration authority and comply with DMS Registration Guidance.
- Ensure adequate training in accordance with the DMS Training Plan.
- Designate DMS Security Officer and site accreditation authority.
- Provide for Certification Authority Workstation (CAW) operations, maintenance, and training.
- Ensure tenant activities are accommodated and appropriate Inter-Service Agreements are in place at both home station and deployable locations.
- Identify the Approving Authorities for Certification Authorities to the National Security Agency (NSA).
- Establish policies, procedures, and doctrine for validating Certification Authority nomination, in coordination with NSA guidelines.
- Designate a single point of contact for coordination.

National Security Agency

- Develop/approve/certify/endorse and ensure availability of security products necessary to ensure secure writer-to-reader messaging services, secure directory services, and secure management services.
- Establish life cycle support for these security products; i.e., an acquisition and life cycle maintenance vehicle, product enhancements, compliance test and evaluation, chair a configuration management board to maintain security product configuration management.
- Provide policies and procedures for the use of these security products.
- Establish and operate the National Security Policy Approving Authority (PAA).
- Establish and operate the National Security Policy Creation Authorities (PCAs).

Designated Acquisition Authority (as assigned by OSD)

- Serve as Executive Agent for the DMS joint acquisition, as directed by ASD(C3I).
- Provide products for implementation of the DMS infrastructure and user desktops as requested.
- Maintain close coordination with Service/Agency DMS Managers, the DMS Program Management Office, and ASD(C3I).

Designated Approval Authorities (DISA, NSA, Joint Staff, and DIA)

- Serve as Designated Approval Authorities for the DMS.
- Designate a single point of contact for coordination.

DEFINITIONS

User Components. All components used by the Military Service and Agency DMS users, to include local enclave connectivity and connectivity to the DISN POP:

User Agents (UAs)	Desktop
Message Stores	Multiple Users
Profiling User Agents	Multiple Users (not mandatory)
CAW	Multiple Users
Local Management Workstations	Multiple Users
FORTEZZA Cards and Readers	Desktop (may also be used for other applications)
Local Mail List Agents	Multiple Users
Subordinate Message Transfer Agent	Multiple Users
Groupware Servers	Multiple Users

Infrastructure Components. Components that support the global messaging infrastructure, including DISN connectivity:

Backbone Message Transfer Agents
Global Directory System Agents
Global Multifunction Interpreters
Global Management Workstations
Global Mail List Agents

NOTE: The actual location of global components will be determined by topological design. Regional deployment of global components is typical.

Requisite Security Products/Services (approved by NSA):

Digital Signature
Encryption Capability
Cryptographic Application Protocol Interfaces
DMS compatible firewalls and guards
Security Management Infrastructure
Certification Authority Workstations

RECOMMENDATIONS FOR DEFENSE INFORMATION INFRASTRUCTURE (DII) NETWORK DII CONNECTION CRITERIA AND ENGINEERING PRACTICES TO ENSURE A ROBUST DEFENSE MESSAGE SYSTEM (DMS)

The DMS is the only messaging system that is consistent with national objectives for interoperable electronic messaging, supporting command and control, administrative, and intelligence information exchange. The DII provides long-haul telecommunications support for the DMS including special purpose networks for the national intelligence community. The Department of Defense (DoD) Components are responsible for facilities, equipment and services necessary to support dissemination, transmission and receipt of messages on their sites (i.e., within the confines of a base/post/camp/station, installation, headquarters, Federal building, or deployable locations).

Component sites support user communities with a range of mission support responsibilities to include critical command and control and combat support messaging. Critical enclaves and users require a high degree of availability and reliability through ready access to pre-designated redundant connectivity, back-up or mirrored system components, high availability or fault tolerant hardware platforms, reliable power, and adequate technical support.

The DMS Initial Operational Test and Evaluation (IOT&E) clearly highlighted the importance of adhering to sound engineering practices when connecting DMS components to the underlying long-haul and base level communications infrastructure. Thereby, the following guidelines will assist in DII and special purpose network connectivity planning to ensure DMS service.

- DMS Subordinate Message Transfer Agents (SMUTS), Local Directory Service Agents (LSD's), mail and/or grouper servers or any other DMS component (such as a Multi-Function Interpreter (MFI), Profiling User Agent (PUA), dedicated Mail List Agent (MLA), etc...) should be a maximum of two router hops away from the closest DII Point of Presence (POP), commonly referred to as a regional or hub router.

- There should be a primary and an alternate telecommunications path to ensure DII/special purpose network connectivity to the DMS site for critical Defense Information Infrastructure (DII) nodes. Alternate DII

ATTACHMENT 3

connectivity can be provided by several different sources, depending on what is available at the DMS site, including other DII router connections already existing at the site, a separate circuit path to a different DII POP, a DII connection provided by another site within the same geographical region, etc. Again, it is recommended that any alternative path be a maximum of two router hops away from a DII POP.

- The primary telecommunications path should be of sufficient capacity as to allow message traffic to pass without delay as well as support a site's composite information technology bandwidth requirements. Formula variables and associated assumptions can be found in the DMS White Paper entitled, "Bandwidth Requirements for DMS at a Site." The electronic version of this document, available on the DMS Home page (http://www.disa.mil/D2/dms/invited/index2.html), includes an embedded Excel worksheet that performs the necessary calculations.

- Total Delay and Availability of the circuit between the DMS site and DII POP are also considerations when determining the telecommunications path, especially for organizational users. These parameters (e.g., an availability objective of 99.975) are provided in "DISA Quality and Reliability Performance Guidelines", (JIEO Engineering Publication 6-95). The criteria identified in this document should be cited when the service is ordered.

- For the majority of cases, the DII should not be part of the local, primary telecommunications path for DMS message traffic destined for a recipient located on the same site as the originator. Site transmission and dissemination facilities should be designed such that local traffic stays within the confines of the site network. There may be certain times when this cannot be avoided (e.g., certain mail list expansions).

- Use of firewalls between the site and the outside world (long haul, regional, wide area networks and local telecommunications systems including DII, Internet, and others) and guards between security enclaves is becoming the norm. The Defense Information Systems Agency, in coordination with the National Security Agency, will maintain and provide current information and reference documents on firewalls and/or guard solutions.